HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200207300-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Art Burget et al.	Confirmation No.:	9679
Application No.:	10/652,010	Examiner:	MOORTHY, Aravind K.
Filing Date:	August 29, 2003	Group Art Unit:	2131

Title: Method and System for Controlling Access of Clients and Users to a Print Server

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on November 11, 2008 .

☐ The fee for filing this Appeal Brief is $540.00 (37 CFR 41.20).

☒ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $130	☐ 2nd Month $490	☐ 3rd Month $1110	☐ 4th Month $1730

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 00 . At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,

Art Burget et al.

By /Steven L. Nichols/

Steven L. Nichols

Attorney/Agent for Applicant(s)

Reg No. : 40,326

Date : April 23, 2009

Telephone : 801-572-8066

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Patent Application of

Art H. Burget et al.

Application No. 10/652,010

Filed: August 29, 2003

For: Method and System for Controlling Access of Clients and Users to a Print Server

Group Art Unit: 2131

Examiner: MOORTHY, Avavind K.

Confirmation No.: 9679

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an Appeal Brief under Rule 41.37 appealing the decision of the Primary Examiner dated September 18, 2008 (the "final Office Action"). Each of the topics required by Rule 41.37 is presented herewith and is labeled appropriately.

I. Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. Related Appeals and Interferences

There are no appeals or interferences related to the present application of which the Appellant is aware.

III. Status of Claims

Claims 5 and 39 have been cancelled previously without prejudice or disclaimer. Thus, claims 1-4, 6-38 and 40-46 are pending in the application and stand finally rejected. Accordingly, Appellant appeals from the final rejection of claims 1-4, 6-38 and 40-46, which claims are presented in the Appendix.

IV. Status of Amendments

A single after-final amendment has been submitted in conjunction with this Brief to correct a minor typographical error in claim 19. Due to the nature of this amendment, i.e., correcting a minor typographical error, it has no impact on the issues presented in this Brief.

V. Summary of Claimed Subject Matter

In general, Appellant has disclosed and claimed a method and system for controlling the source of print job requests to a printer or print server is described herein. The disclosed subject matter uses a key distribution process to control which clients have permissions to send print job requests to a printer or print server. In an additional embodiment, the key distribution process controls which users of a specific client have permission to send print job requests to a printer print server. (*Appellant's specification , paragraph 0017*).

Turning to the specific language and elements of the claims, Appellant's claimed subject matter is as follows.

1. A method of controlling use of a printer on a network, said method comprising:

with a print server (100), generating (120) a key for a specific client (103) of said print server (*Appellant's specification, paragraph 0025*);

embedding (121) said key in a printer driver (*Appellant's specification, paragraph 0030*);

providing (123) said key to said specific client on said network by installing said printer driver on said specific client (*Appellant's specification, paragraph 0031*), wherein said key is used to submit a print job from said client to a printer on said network (*Appellant's specification, paragraph 0031*).

13. A method of controlling a user's ability to cause a client to send a print job to a printer, said method comprising providing (153) said client with a key specifically configured for said user (*Appellant's specification, paragraph 0048*), wherein said client will refuse

(160, 161) to submit a print job to said printer for a particular user unless said key associated with that user has been provided to said client (*Appellant's specification, paragraph 0050*).

19. A system for controlling a client's ability to send a print job to a printer on a network, said system comprising:

at least one client (103) (*Appellant's specification, paragraph 0018*);

a print server (100) for managing distribution of print jobs to one or more printers (102) (*Appellant's specification, paragraph 0019*); and

a network (101) connecting said at least one client device, said print server and said one or more printers (*Appellant's specification, paragraph 0018*);

wherein said print server (100) generates a key for a specific client of said print server (*Appellant's specification, paragraph 0025*), embeds said key in a printer driver (*Appellant's specification, paragraph 0030*); and installs said printer driver on said specific client (*Appellant's specification, paragraph 0031*), said printer server then requires said specific client to use said key provided to said client when said client is submitting a print job to said print server (133-135) (*Appellant's specification, paragraph 0034*).

30. A system for controlling a user's ability to cause a client to print a print job to a printer on a network, said system comprising:

a client (103) (*Appellant's specification, paragraph 0018*); and

a print server (100) for managing at least one network printer (102) (*Appellant's specification, paragraph 0019*), wherein said print server (100) provides a key to said client (103) for use in submitting a print job, said key being specific to a particular user of said client(*Appellant's specification, paragraph 0031*);

wherein said client (103) will refuse (160, 161) to submit a print job for a user unless said client has been previously provided with a key specific to that user (*Appellant's specification, paragraph 0050*).

38. A system controlling use of a printer on a network, said system comprising:

a client (103) connected to said network (101) for generating a print job for said printer (102) (*Appellant's specification, paragraph 0018*);

means (100) for providing a key to said client (103), wherein said key is specific to a user of said client and is used to encrypt a print job from said client to said printer (*Appellant's specification, paragraph 0025*); and

means on said client (103) for encrypting said print job using said key to produce an encrypted print job for transmission to said printer (102) (*Appellant's specification, paragraph 0050*).

VI. Grounds of Rejection to be Reviewed on Appeal

The final Office Action raised the following grounds of rejection.

(1) Claims 13-18, 30-38 and 40-46 were rejected under 35 U.S.C. §102(b) as anticipated by U.S. Patent No. 7,305,556 to Slick ("Slick").

(2) Claims 1-4, 6-10 and 19-29 were rejected under 35 U.S.C. § 103(a) over the combined teachings of Slick and U.S. Patent App. Pub. No. 2002/0169002 to Imbrie et al. ("Imbrie").

According, Appellant hereby requests review of each of these grounds of rejection in the present appeal.

VII. Argument

(1) Claims 13-18, 30-38 and 40-46 are patentable over Slick:

Claim 13:

Independent claim 13 recites:

> A method of controlling a user's ability to cause a client to send a print job to a printer, said method comprising providing said client with a key specifically configured for said user, wherein said client will refuse to submit a print job to said printer for a particular user unless said key associated with that user has been provided to said client.

Applicant wishes to point out that claim 13 recites that the "client will refuse to submit a print job ... for a particular user unless [a] key associated with that user has been provided to said client." This subject matter is not taught or suggested by Slick.

In this regard, the Office Action cites to Slick at col. 12, lines 1-23. (Action, p. 4). However, this portion of Slick does not teach or suggest the claimed method in which a client is to be provided with a key "*specifically configured for [a particular] user*" and where the client will *refuse* to submit a print job for that particular user unless the key associated with that particular user has been provided to the client.

The cited portion of Slick, which refers to Fig. 8, describes a method of securing a printer public key by encryption. The printer public key is encrypted with a user-specific private key. (Slick, Fig. 8A, S805). However, in the teachings of Slick, the user-specific key is always available. There is never any question of whether the user-specific key has been provided. Consequently, Slick does not teach the claimed method in which "said client will refuse to submit a print job to said printer for a particular user *unless said key associated with that user has been provided to said client.*" (Emphasis added). This subject matter is entirely outside the scope and content of Slick.

In light of this argument, the final Office Action now also refers to Slick at Fig. 5A in attempting to reject claim 13. (Action, p. 2). According to the Action, this figure depicts the claimed subject matter of the client refusing to submit a print job for a particular use unless a key associated with that user has been provided to the client. (*Id.*). However, in Fig. 5A and the related text, the user-specific private key (53), *which is always available*, is merely used in a decryption algorithm (76) to decrypt a printer public key stored by the client. Again, Slick does not ever teach or suggest that the user-specific private key (53) is or is not provided to a client or that the client will refuse to submit a print job "for a particular user unless said key associated with that user has been provided to said client." (Claim 13). Rather, Slick merely teaches that, if the printer public key has been corrupted, the user is prompted to obtain a new copy of the printer public key. (Slick, col. 9, lines 44-47). This does not mean that the client refuses to submit a print job as recited in claim 13. Rather, in the Slick system the user may still submit the print job without encrypting the print data or may obtain a new copy of the printer public key and submit the print job. There is no connection to whether or not a key specifically configured for a particular user has or has not been provided in connection with the print job. Slick simply does not teach or suggest, as recited in claim 13, that the "client will refuse to submit a print job to said printer for a particular user unless said key associated with that user has been provided to said client."

"A claim is anticipated [under 35 U.S.C. § 102] only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987). See M.P.E.P. § 2131. Therefore, for at least the reasons explained here, the rejection based on Slick of claim 13 and its dependent claims should be reconsidered and withdrawn.

Claim 30:

Independent claim 30 recites:

> A system for controlling a user's ability to cause a client to print a print job to a printer on a network, said system comprising:
> a client; and
> a print server for managing at least one network printer, wherein said print server provides a key to said client for use in submitting a print job, said key being specific to a particular user of said client;
> *wherein said client will refuse to submit a print job for a user unless said client has been previously provided with a key specific to that user.*

(Emphasis added).

However, as demonstrated above with respect to claim 13, in the teachings of Slick, the user-specific key is always available. There is never any question so whether the user-specific key has been provided. Consequently, Slick does not teach or suggest the claimed method in which "said client will refuse to submit a print job to said printer for a particular user *unless said key associated with that user has been provided to said client.*" (Emphasis added). This subject matter is entirely outside the scope and content of Slick.

"A claim is anticipated [under 35 U.S.C. § 102] only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987). See M.P.E.P. § 2131. Therefore, for at least the reasons explained here, the rejection based on Slick of claim 30 and its dependent claims should be reconsidered and withdrawn.

Claim 38:

Independent claim 38 recites:

> A system controlling use of a printer on a network, said system comprising:
> a client connected to said network for generating a print job for said printer;

means for providing a key to said client, wherein said key is specific to a user of said client and is *used to encrypt a print job* from said client to said printer.

means on said client for encrypting said print job using said key to produce an encrypted print job for transmission to said printer.

(Emphasis added).

In contrast, as demonstrated above, Slick only teaches the use of user-specific keys for securing other keys. Slick does not teach or suggest a system as recited in claim 38 with means for providing a key to a client *that is specific to a user of that client* and is used to encrypt print jobs from that client to a printer.

In this regard, the Action cites, Slick at col. 10. (Action, p. 8). However, that portion of Slick teaches that the client uses a "random key generator" to generate a "symmetric key, which is a cryptographic key that can be used to encrypt and to decrypt a data object." This randomly generated symmetric key is then used to encrypt the print data that is sent to the printer. *However, nowhere does Slick teach or suggest that this randomly generated symmetric key is specific to a particular user of the client.* The "printer public key 75" is used to encrypt the symmetric key, as the "printer 20 will need a secure copy of symmetric key 83 to decrypt encrypted print data 87 for printing" (Slick, col. 10, lines 16-37). Thus, the randomly generated symmetric key is used to encrypt the print data that is sent to the printer. Clearly, the symmetric key used to encrypt the print data as taught by Slick is not a key specific to a particular user as recited in claim 38.

In the final Office Action, the Examiner responds to this argument (Action, pp. 3-4) by reiterating the same teachings from Slick. The final Office Action does not address, however, the clear fact that the *random* key (83) is *not* specific to a particular user of the client. Rather, a new random key (83) is generated by the random key generator (82) for each print job (Slick, Fig. 6) and is not the claimed key that "is specific to a user of said client." (Claim 38).

"A claim is anticipated [under 35 U.S.C. § 102] only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987). See M.P.E.P. § 2131. Therefore, for at least the reasons explained here, the rejection based on Slick of claim 38 and its dependent claims should be reconsidered and withdrawn.

Claims 6 and 15:

Additionally, various dependent claims of the application recite subject matter that is further patentable over the cited prior art. Specific, non-exclusive examples follow.

Dependent claims 6 and 15 disclose "storing a related key on a storage device of said print server." In response, the Action cites to Slick, column 8 lines 9-17, which teach that a "storage area 62 includes printer public key." When examined in context, it becomes readily apparent that "storage area 62" is "a general storage area of fixed disk 13," (column 8, lines 9-17) which is described as one of the internal contents of "computer 10" (Slick, column 6, lines 22-24). Computer 10 is analogous to the client disclosed in claim 14, and not the print server. Thus, nowhere does Slick teach or suggest that the related key is stored "on a storage device of said print server" (claims 6, 15).

(2) Claims 1-4, 6-10 and 19-29 are patentable over Slick and Imbrie:

Claim 1:

Independent claim 1 now recites

> A method of controlling use of a printer on a network, said method comprising:
> with a print server, generating a key for a specific client of said print server;

embedding said key in a printer driver;

providing said key to said specific client on said network by installing said printer driver on said specific client, wherein said key is used to submit a print job from said client to a printer on said network.

(Emphasis added.)

According to the final Office Action, Slick "discloses a method of controlling use of a printer on a network, the method comprising: with a print server, generating a key for a specific client of the print server; wherein the key is used to submit a print job from the client to a printer on the network [column 6, lines 37-49]." (Action, p. 9). This, however, is a mischaracterization of what Slick actually teaches.

The cited portion of Slick, in its entirety, reads as follows.

> Printer public key 25 is made accessible to the public for use in the encryption of print data to send to printer 20 in a secure, encrypted manner. Printer private key 23 is also a cryptographic key which corresponds to printer public key 25, and is also created by the creator of printer public key 25. However, unlike printer public key 25, printer private key 23 is maintained under strict security within printer 20 and cannot be accessed and/or removed from printer 20. In this manner, only printer 20 has access to both of keys 23 and 25 of printer key pair 22, thereby allowing users of printer 20 to trust that encrypted print data sent to printer 20 cannot be decrypted by any unauthorized party if the encrypted print data should be intercepted on its way to printer 20.

(Slick, col. 6, lines 37-49).

Consequently, Slick does no teach or suggest "generating a key for a specific client of the print server" as recited in claim 1. Rather, Slick merely recites ***one*** printer public key that is provided to all authorized users of the printer with which to encrypt print data being sent to the printer. This teaches away from "generating a key *for a specific client* of the print server" as recited in claim 1. (Emphasis added).

Additionally, Slick does not teach or suggest that "generating a key for a specific client of the print server" is performed "with a print server" as also recited in claim 1. Thus, Slick clearly fails to teach or suggest the features of claim 1 for which it, Slick, was cited by the final Office Action.

Imbrie, likewise, fails to teach or suggest "with a print server, generating a key for a specific client of said print server." Consequently, Imbrie does not and cannot remedy the deficiencies of Slick. Thus, the combination of Slick and Imbrie utterly fails to teach or suggest, "with a print server, generating a key for a specific client of said print server," as recited in claim 1.

The combination of Slick and Imbrie further fails to teach or suggest "embedding said key in a printer driver; providing said key to said specific client on said network by installing said printer driver on said specific client." The final Office Action fails to indicate how or where the cited prior art teaches that a client-specific key is provided to that client "by installing [a] printer driver on said specific client." This subject matter is entirely absent from the cited prior art.

The combination of Slick and Imbrie further fails to teach or suggest that a key embedded in a printer driver "is used to submit a print job from said client to a printer on said network" as recited in claim 1. The final Office Action cited Imbrie at paragraph 0037 as teaching a printer driver in which an encryption key is embedded. (final Office Action, p. 9). According to the final Office Action, "Imbrie et al teaches permitting encryption/decryption of data received from the intermediate device, a public key can be provided and embedded within the print driver for use with a later generated private key to encrypt or decrypt data pockets transmitted from the printing assembly 40 [0037]." (Action, p. 9).

However, as correctly indicated by the final Office Action, the public key taught by Imbrie is used by a "submitting device" (Imbrie, paragraph 0037), which is the printer client, to receive data "from the printing assembly 40" (*Id.*). Thus, Imbrie teaches a public key that is used to transmitted encrypted data from the printer or printing assembly to the client or submitting device. This is the exact opposite of claim 1 which recites that the embedded is

key "used to submit a print job from said client to a printer on said network." Consequently, the combination of Slick and Imbrie further fails to teach or suggest that a key embedded in a printer driver "is used to submit a print job from said client to a printer on said network" as recited in claim 1. Given all these features of claim 1 that are not taught or suggested by the cited prior art, claim 1 is clearly beyond the scope and content of the cited prior art.

The Supreme Court recently addressed the issue of obviousness in *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727 (2007). The Court stated that the *Graham v. John Deere Co. of Kansas City*, 383, U.S. 1 (1966), factors still control an obviousness inquiry. Under the analysis required by *Graham v. John Deere*, 383 U.S. 1 (1966) to support a rejection under § 103, the scope and content of the prior art must first be determined, followed by an assessment of the differences between the prior art and the claim at issue in view of the ordinary skill in the art. In the present case, the scope and content of the prior art, as evidenced by Slick and Imbrie, did not include the claimed subject matter, particularly a method that includes, "with a print server, generating a key for a specific client of said print server; embedding said key in a printer driver; providing said key to said specific client on said network by installing said printer driver on said specific client, wherein said key is used to submit a print job from said client to a printer on said network." As demonstrated above, the final Office Action has failed to correctly assesses the differences between the cited prior art and claimed subject matter.

The differences between the cited prior art and the claimed subject matter are significant because, as demonstrated above, the claimed subject matter provides features and advantages not known or available in the cited prior art. Consequently, the cited prior art will not support a rejection of claim 1 and its dependent claims under 35 U.S.C. § 103 and *Graham*.

Claim 19:

Claim 19 recites:

> A system for controlling a client's ability to send a print job to a printer on a network, said system comprising:
> at least one client;
> a print server for managing distribution of print jobs to one or more printers; and
> a network connecting said at least one client device, said print server and said one or more printers;
> wherein said print server generates a key for a specific client of said print server, embeds said key in a printer driver; and installs said printer driver on said specific client, said printer server than requires said specific client to use said key provided to said client when said client is submitting a print job to said print server.

Like claim 1 above, claim 19 recites a system that comprises at least one client and a print server managing distribution of print jobs to one or more printers "wherein said print server generates a key for a specific client of said print server, embeds said key in a printer driver; and installs said printer driver on said specific client, said printer server then requires said specific client to use said key provided to said client when said client is submitting a print job to said print server." As demonstrated above, the combination of Slick and Imbrie does not teach or suggest the claimed print server that "generates a key for a specific client of said print server, embeds said key in a printer driver; and installs said printer driver on said specific client."

Claim 19 further recites that the "print server," as opposed to some other constituent of the system, "requires said specific client to use said key provided to said client when said client is submitting a print job to said print server." All this subject matter is clearly outside the scope and content of the cited prior art.

As noted above, the Supreme Court recently addressed the issue of obviousness in *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727 (2007). The Court stated that the *Graham v.*

John Deere Co. of Kansas City, 383, U.S. 1 (1966), factors still control an obviousness inquiry. Under the analysis required by *Graham v. John Deere*, 383 U.S. 1 (1966) to support a rejection under § 103, the scope and content of the prior art must first be determined, followed by an assessment of the differences between the prior art and the claim at issue in view of the ordinary skill in the art. In the present case, the scope and content of the prior art, as evidenced by Slick and Imbrie, did not include the claimed subject matter, particularly a system in which a "print server generates a key for a specific client of said print server, embeds said key in a printer driver; and installs said printer driver on said specific client, said printer server then requires said specific client to use said key provided to said client when said client is submitting a print job to said print server." As demonstrated above, the final Office Action has failed to correctly assesses the differences between the cited prior art and claimed subject matter.

The differences between the cited prior art and the claimed subject matter are significant because, as demonstrated above, the claimed subject matter provides features and advantages not known or available in the cited prior art. Consequently, the cited prior art will not support a rejection of claim 19 and its dependent claims under 35 U.S.C. § 103 and *Graham*.

In view of the foregoing, it is submitted that the final rejection of the pending claims is improper and should not be sustained. Therefore, a reversal of the Rejection of September 18, 2008 is respectfully requested.

Respectfully submitted,

DATE: April 23, 2009

/Steven L. Nichols/
Steven L. Nichols
Registration No. 40,326

Steven L. Nichols, Esq.
Managing Partner, Utah Office
Rader Fishman & Grauer PLLC
River Park Corporate Center One
10653 S. River Front Parkway, Suite 150
South Jordan, Utah 84095
(801) 572-8066
(801) 572-7666 (fax)

VIII. CLAIMS APPENDIX

1. (previously presented)A method of controlling use of a printer on a network, said method comprising:

with a print server, generating a key for a specific client of said print server;

embedding said key in a printer driver;

providing said key to said specific client on said network by installing said printer driver on said specific client, wherein said key is used to submit a print job from said client to a printer on said network.

2. (original) The method of claim 1, further comprising using said key to encrypt said print job on said client prior to transmission of said print job to said printer.

3. (original) The method of claim 2, further comprising using said key or a related key to decrypt said print job for use by said printer.

4. (original) The method of claim 1, wherein said key is specific to a particular user, said method further comprising using said key to submit said print job from said client device only at the request of said particular user.

5. (cancelled)

6. (previously presented) The method of claim 1, further comprising:

storing a related key on a storage device of said print server .

7. (original) The method of claim 6, further comprising:

encrypting said print job with said key resulting in an encrypted print job;

sending said encrypted print job from said client to said print server; and

attempting to decrypt said encrypted print job with said related key stored on said storage device of said print server;

wherein, if said related key correctly matches said key used to generate said encrypted print job, said print server successfully decrypts said encrypted print job and causes said printer to print said print job.

8. (previously presented)The method of claim 1, wherein installing said driver further comprises re-installing said driver with said key on said client if a driver without said key is already installed on said client.

9. (previously presented)The method of claim 1, wherein installing said driver further comprises re-configuring said driver on said client with said key if a driver without said key is already installed on said client.

10. (previously presented)The method of claim 1, wherein installing said driver with said key further comprises installing said key on said client without installing said driver if a driver configured to use said key is already installed on said client.

11. (previously presented)The method of claim 1, wherein said key allows said client to print to multiple networked printers managed by said print server.

12. (previously presented)The method of claim 1, wherein said key is provided to multiple clients.

13. (original) A method of controlling a user's ability to cause a client to send a print job to a printer, said method comprising providing said client with a key specifically configured for said user, wherein said client will refuse to submit a print job to said printer for a particular user unless said key associated with that user has been provided to said client.

14. (original) The method of claim 13, further comprising:

generating said key with a print server; and

transmitting said key to said client from said print server over a network to which said print server, client and printer are all connected.

15. (original) The method of claim 14, further comprising:

storing a related key on a storage device of said print server;

associating said key with a printer driver for said printer; and

installing said driver with said associated key on said client.

16. (original) The method of claim 15, further comprising:

encrypting said print job with said key resulting in an encrypted print job;

sending said encrypted print job to said print server; and

attempting to decrypt said encrypted print job with said related key on said storage device of said print server;

wherein, if said related key correctly matches said key used to generate said encrypted print job, said print server successfully decrypts said encrypted print job and causes said printer to print said print job.

17. (original) The method of claim 14, wherein said key allows said user to cause said client to print to multiple networked printers managed by said print server.

18. (original) The method of claim 13, wherein said key is provided to multiple clients.

19. (previously presented) A system for controlling a client's ability to send a print job to a printer on a network, said system comprising:

at least one client;

a print server for managing distribution of print jobs to one or more printers; and

a network connecting said at least one client device, said print server and said one or more printers;

wherein said print server generates a key for a specific client of said print server, embeds said key in a printer driver; and installs said printer driver on said specific client, said printer server than requires said specific client to use said key provided to said client when said client is submitting a print job to said print server.

20. (previously presented)The system of claim 19, wherein said print server is configured to:

generate said key with a utility; and

store a related key on a storage device.

21. (original) The system of claim 20, wherein said client is configured to:

encrypt said print job with said key resulting in an encrypted print job; and

send said encrypted print job to said print server;

said printer server being further configured to attempt to decrypt said encrypted print job with said related key stored on said storage device.

22. (original) The system of claim 21, wherein, if said related key correctly matches said key used to generate said encrypted print job, said print server successfully decrypts said encrypted print job and causes said printer to print said print job.

23. (original) The system of claim 19, wherein said key allows said client to print to multiple printers managed by said print server.

24. (original) The system of claim 19, wherein said key is provided to multiple clients.

25. (original) The system of claim 19, wherein said key allows any user to cause said client to send said print job to said print server.

26. (original) The system of claim 19, wherein said at least one client comprises a personal computer.

27. (original) The system of claim 20, wherein said configuration utility is an embedded web server that resides on said print server.

28. (original) The system of claim 20, wherein said storage device is incorporated into said print server.

29. (original) The system of claim 20, wherein said storage device is connected to said network, but separate from said print server.

30. (original) A system for controlling a user's ability to cause a client to print a print job to a printer on a network, said system comprising:

a client; and

a print server for managing at least one network printer, wherein said print server provides a key to said client for use in submitting a print job, said key being specific to a particular user of said client;

wherein said client will refuse to submit a print job for a user unless said client has been previously provided with a key specific to that user.

31. (original) The system of claim 30, wherein said print server comprises:

a configuration utility for configuring said key; and

a storage device for storing a related key.

32. (original) The system of claim 31, wherein said print server:

configures said key specifically for said user with said configuration utility;

stores a related key on said storage device;

associates said key with a printer driver for said printer; and

installs said key in association with said driver on said client.

33. (original) The system of claim 32, wherein said user causes said client to:

encrypt said print job with said key resulting in an encrypted print job; and

send said encrypted print job to said print server;

said print server being configured to attempt to decrypt said encrypted print job with said related key stored on said storage device.

34. (original) The system of claim 33, wherein, if said related key correctly matches said key used to generate said encrypted print job, said print server successfully decrypts said encrypted print job and causes said printer to print said print job.

35. (original) The system of claim 30, wherein said key allows said user to cause said client to print to multiple printers managed by said print server.

36. (original) The system of claim 30, wherein said key is provided to multiple clients.

37. (original) The system of claim 31, wherein said configuration utility is an embedded web server that resides on said print server.

38. (previously presented)A system controlling use of a printer on a network, said system comprising:

a client connected to said network for generating a print job for said printer;

means for providing a key to said client, wherein said key is specific to a user of said client and is used to encrypt a print job from said client to said printer; and

means on said client for encrypting said print job using said key to produce an encrypted print job for transmission to said printer.

39. (cancelled)

40. (original) The system of claim 38, further comprising decryption means for using a related key to decrypt said print job for use by said printer.

41. (original) The system of claim 40, wherein said decryption means comprise a printer server.

42. (original) The system of claim 38, wherein said key is used by multiple clients on said network.

43. (previously presented)The system of claim 38, wherein said client is configured to use said key to submit said print job only at the request of said particular user.

44. (original) The system of claim 38, wherein said means for providing a key comprise a print server on said network.

45. (original) The system of claim 44, wherein said printer server further comprises:

means for storing a related key on a storage device of said print server;

means for associating said key with a printer driver for said printer; and

means for installing said key in association with said printer driver on said client.

46. (original) The system of claim 45, wherein said printer server further comprises:

means for attempting to decrypt said encrypted print job with a related key;

wherein, if said related key correctly matches said key used to generate said encrypted print job, said print server successfully decrypts said encrypted print job and causes said printer to print said print job.

IX. Evidence Appendix

None

X. Related Proceedings Appendix

None